EXHIBIT A

Notice of Data Privacy Event

October 24, 2023 – Welltok, Inc. ("Welltok") is providing notice of an event that may affect the privacy of certain individuals' information. Welltok takes this incident very seriously and is providing information about the incident, our response to it, and resources available to individuals to help protect their information, should they feel it appropriate to do so.

What Happened? On July 26, 2023, Welltok was alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool. Welltok had previously installed all published patches and security upgrades immediately upon such patches being made available by Progress Software, the developer of the MOVEit Transfer tool. Welltok also conducted an examination of our systems and networks using all information available to determine the potential impact of the vulnerabilities we were alerted to on the MOVEit Transfer server and the security of data housed on the server, and confirmed that there was no indication of any compromise at that time.

Welltok continued to investigate this issue using the assistance of third-party cybersecurity specialists and additional information that had been discovered in the intervening period to determine the potential for hidden vulnerabilities on the MOVEit Transfer server and assess the security of data housed on the server. After a full reconstruction of our systems and historical data, the investigation determined on August 11, 2023 that an unauthorized actor exploited software vulnerabilities, accessed the MOVEit Transfer server on May 30, 2023, and exfiltrated certain data from the MOVEit Transfer server during that time. Welltok subsequently undertook a time-consuming and detailed reconstruction and review of the data stored on the server at the time of this incident to understand the contents of that data and to whom that data relates. Subsequently, on August 26, 2023, Welltok learned that data related to certain individuals was present on the impacted server at the time of the event.

We are providing notice to impacted individuals on behalf of the following organizations:

- Asuris Northwest Health
- BridgeSpan Health
- Blue Cross and Blue Shield of Minnesota and Blue Plus

- Blue Cross and Blue Shield of Alabama
- Blue Cross and Blue Shield of Kansas
- Blue Cross and Blue Shield of North Carolina
- CHI Health – NE
- CHI Memorial – TN
- CHI Memorial – GA
- CHI St. Joseph Health
- CHI St. Luke's Health Brazosport
- CHI St. Luke's Health Memorial
- CHI St. Vincent
- Corewell Health
- Faith Regional Health Services
- Horizon Blue Cross Blue Shield of New Jersey
- Hospital & Medical Foundation of Paris, Inc. dba Horizon Health
- Marshfield Clinic Health System
- Mass General Brigham Health Plan
- Mercy Health
- Priority Health
- Regence BlueCross BlueShield of Oregon
- Regence BlueShield
- Regence BlueCross BlueShield of Utah
- Regence Blue Shield of Idaho
- St. Bernards Healthcare
- St Joseph Health
- St. Alexius Health
- St. Luke's Health
- Sutter Health
- Trane Technologies Company LLC and/or group health plans sponsored by Trane Technologies Company LLC or Trane U.S. Inc.
- Trinity Health
- The group health plans of Stanford Health Care, of Stanford Health Care, Lucile Packard Children's Hospital Stanford, Stanford Health Care Tri-Valley, Stanford Medicine Partners, and Packard Children's Health Alliance
- The Guthrie Clinic
- Virginia Mason Franciscan Health

What Information Was Involved? While we have no evidence that any of your information has been misused, we are notifying you and providing information and resources to help protect your personal information. The

following types of information may have impacted: name and address, telephone number, email address. The type of information at issue varies for each person. For a small group of impacted clients, Social Security Numbers, Medicare/Medicaid ID Numbers, or certain Health Insurance information such as plan or group name, were also implicated. For other individuals, certain health information such as a provider name, prescription name, or treatment code may have been included.

What We Are Doing. We take this event and the security of personal information in our care very seriously. Upon learning of this event, we moved quickly to investigate and respond to the event and notify potentially affected individuals. As part of our ongoing commitment to the security of information, we are reviewing and enhancing our existing policies and procedures related to data privacy to reduce the likelihood of a similar future event. We are notifying impacted individuals for whom a valid mailing address is available via U.S. mail and offering them credit monitoring and identity protection services. We are also notifying applicable regulators.

How Will Individuals Know If They Are Affected By This Incident? Welltok is mailing a notice letter to individuals whose information was determined to be in the affected files, for whom we have a valid mailing address. If an individual does not receive a letter but would like to know if they are affected, they may call our dedicated assistance line, detailed below.

What You Can Do. We encourage individuals to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits forms, and monitoring your free credit reports for suspicious activity and to detect errors. Under U.S. law individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report, place a fraud alert, or a security freeze. Contact information for the credit bureaus is below:

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control

over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you may need to provide the following information, depending on whether the request is made online, by phone, or by mail:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their

information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 1-202-727-3400; and oag.dc.gov. (mailto:oag@dc.gov)

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/. (https://www.marylandattorneygeneral.gov/)

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra (http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra).pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/. (https://ag.ny.gov)

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov. (http://www.ncdoj.gov/)

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov (http://www.riag.ri.gov/). Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

For More Information. If individuals have questions or would like additional information, they may call Welltok's dedicated assistance line at 800-628-2141 between the hours of 6:00 a.m. and 8:00 p.m. Pacific Time, Monday through Friday, and on Saturday and Sunday between the hours of 8:00 a.m. to 5:00 p.m. Pacific Time excluding major U.S. holidays. Be prepared to provide engagement number B107737.